

CLAIMS

Having thus described our invention, what we claim as new, and desire to secure by Letters Patent is:

Sub
B1

1 1. A method for securely handling an information
2 unit by a first information processing device
3 (2) interoperating with a second secure
4 information processing device (1), in
5 particular a chip card, whereby the information
6 unit is provided by an issuer,

7
8 the method comprising the steps:

9 providing (3, 25, 35) the information unit from
10 the issuer to the first information processing
11 device (2), the information unit being
12 processed by a cryptographic process;

13
14 providing at least one key for the
15 cryptographic process on the second secure
16 information processing device (1); and

17
18 cryptographically reprocessing (29, 38) the
19 information unit by using the at least one key.

1 2. The method according to claim 1, comprising:

2 providing (3, 25, 35) the information unit from
3 the issuer to the first information processing
4 device (2), the information unit being
5 encrypted by using at least a first key;

66000-00000

6 providing the first key from the issuer to the
7 first information processing device (2), the
8 first key being encrypted by using at least a
9 second key;

10
11 providing the at least one second key on the
12 second secure information processing device
13 (1);

14
15 interconnecting the first information
16 processing device (2) and the second secure
17 information processing device (1);

18 on side of the second secure information
19 processing device, decrypting (27) the at least
20 first key by using the at least second key; and

21
22 decrypting (29) the information unit by using
23 the decrypted at least first key.

1 3. The method according to claim 1, comprising:

2 providing (3, 25, 35) the information unit from
3 the issuer to the first information processing
4 device (2), the information unit being signed
5 by using a signature;

6 providing the signature from the issuer to the
7 first information processing device (2), the
8 signature being generated by using at least one
9 key;

10

1 6. The method according to claim 5, wherein the
2 encrypted information unit, the encrypted first
3 key, and/or the signature key, and/or the
4 generated signature, and/or the control command
5 are downloaded (25, 35) from a central server
6 (4) .

1 7. The method according to claim 3, wherein the
2 second key and/or the key for signature
3 verification are/is securely stored on the
4 second secure device (1) at time of its issuing
5 by the issuer.

1 8. The method according to claim 2, wherein at
2 least a third key is provided for external
3 authentication and/or release control of the
4 respective information unit.

1 9. The method according to claim 8, wherein the
2 first device (2) is initiated to gather a new
3 release of the information unit from the
4 issuer, depending on the respective status of
5 the third key.

1 10. The method according to claim 9, wherein the
2 new release of the information unit is
3 downloaded from an internet server (4) provided
4 by the issuer.

1 11. The method according to claim 2, wherein the at
2 least first key and/or the signature are/is
3 randomized between different sessions of

providing the information unit from the issuer to the first device (2).

12. The method according to claim 1, wherein the first information processing device (2) is a terminal device, and the second secure information processing device (1) is a portable device.

13. The method according to claim 12, wherein the terminal device is a chip card reader and the portable device is a chip card.

14. A system for securely handling an information unit, comprising a first information processing device (2) interoperating with a second secure information processing device (1), in particular a chip card, the information unit being provided by an issuer,

comprising:

the first device (2) comprising
a storage for storing the information
unit; and

the second secure device (1) comprising
a storage (6) for storing at least one key
for a cryptographic process; and

15 providing means for cryptographically
16 reprocessing the information unit by using the
17 at least one key.

1 15. The system according to claim 14, wherein
2 the first device (2) comprises
3 a storage for storing the information
4 unit, encrypted by using at least a first
5 key, and a storage for storing the first
6 key, encrypted by using at least a second
7 key;
8 the second secure device (1) comprises
9 a storage (6) for storing the at least one
10 second key, and processing means for
11 decrypting the at least first key by using
12 the at least second key; and
13 providing means for decrypting the information
14 unit by using the decrypted at least first key.

1 16. The system according to claim 14, wherein
2 the first device (2) comprises
3 a storage for storing the information unit
4 and a signature for the information unit;
5
6 the second secure device (1) comprises
7 a storage (6) for storing at least one
8 signature key;

5000-22000

4 information processing device (1) is a portable
5 device.

1 27. The system according to claim 26, wherein the
2 terminal device is a chip card reader and the
3 portable device is a chip card.

1 28. A chip card (1) for securely handling an
2 information unit by interoperating with an
3 information handling terminal device (2),
4 comprising a storage (6) for storing an at
5 least one key for the cryptographic process.

1 29. The chip card according to claim 28, wherein
2 processing means (7) performing an access
3 control is controlled by an information unit.

1 30. The chip card according to claim 28, wherein a
2 processor (7) runs specific functions on the
3 terminal device (2, 5) or on at least a second
4 device attached to the terminal device (2, 5).

1 31. The chip card according to claim 28, further
2 comprising means for transferring of the at
3 least one second key to the terminal device (2,
4 5) and/or means for decrypting of the at least
5 first key by using the at least second key
6 and/or means to initiate transfer of the
7 signature key for signature verification.

1 38. The chip card accepting device according to
2 claim 37, further comprising means for
3 downloading the encrypted information unit, the
4 at least one key and the digital signature from
5 a central server (4).

1 39. The chip card accepting device according to
2 claim 35, further comprising a storage for
3 storing at least a third key for external
4 authentication and/or release control of the
5 information unit and processing means for
6 processing the third key.

1 40. The chip card accepting device according to
2 claim 39, further comprising means to initiate
3 download of a new release of the information
4 unit, depending on the respective status of the
5 third key.